Astra Linux

Astra Linux

S – -: , VipNet . .

Lite – -: , VipNet . . CCID

2.0 – . () , — , . 2012. . 2016 . .

PKI 3.0

: https://dev.rutoken.ru/pages/viewpage.action?pageId=66814078

Astra Linux:

, .

Lite/S :

1) eSign
2) csptestf CSP. « CSP»

2.0 :

1) eSign
2) +
3) OpenSSL + engine
4) csptestf CSP. « CSP»

Lite , USB-.
:
1) +
2) CSP 5.0

:

- libccid, librtpkcs11ecp.so;
- libpcsclite1 pcscd;
- opensc;
- pcsc-tools.

:

```
sudo apt install libccid pcscd libpcsclite1 pcsc-tools opensc
```

librtpkcs11ecp.so :
https://www.rutoken.ru/support/download/pkcs/

Библиотека rtPKCS11ecp для GNU/Linux DEB 32-bit (x86)

Версия: v.1.8.2.0 от 02.03.2018

Поддерживаемые ОС: 32-разрядные Debian/Ubuntu/Mint/Astra

Библиотека rtPKCS11ecp для GNU/Linux DEB 64-bit (x64)

Версия: v.1.8.2.0 от 02.03.2018

Поддерживаемые ОС: 64-разрядные Debian/Ubuntu/Mint/Astra

```
sudo apt install ./librtpkcs11ecp_1.8.2.0-1_amd64.deb
```

:
.

1

:

```
pcsc_scan
```

```
Tue Oct 16 14:49:45 2018
Reader 0: Aktiv Rutoken ECP 00 00
  Card state: Card inserted,
  ATR: 3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1

ATR: 3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1
+ TS = 3B --> Direct Convention
+ T0 = 8B, Y(1): 1000, K: 11 (historical bytes)
  TD(1) = 01 --> Y(i+1) = 0000, Protocol T = 1
-----
+ Historical bytes: 52 75 74 6F 6B 65 6E 20 44 53 20
  Category indicator byte: 52 (proprietary format)
+ TCK = C1 (correct checksum)

Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1
        Rutoken ECP (DS)
```

2

:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -T
```

```
root@smakhmadiev:/home/shuhrat/ecp# pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -T
Available slots:
Slot 0 (0x0): Aktiv Rutoken ECP 00 00
  token label        : Rutoken ECP <no label>
  token manufacturer : Aktiv Co.
  token model        : Rutoken ECP
  token flags        : rng, login required, PIN initialized, token initialized, user PIN
  hardware version   : 20.5
  firmware version   : 23.2
  serial num         : 390a75ab
```

librtpkcs11ecp.so

librtpkcs11ecp.so :

```
find /usr/*(lib|lib64) -name librtpkcs11ecp.so
```

3

XCA:

XCA:

PIN-

pin- :

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so --login --pin __ --change-pin
--new-pin __
```

, PIN- :

```
Using slot 0 with a present token (0x0)
PIN successfully changed
```

:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -O -l
```

, :

```
Using slot 0 with a present token (0x0)

Public Key Object; RSA 2048 bits
  label:      Test
  ID:         45
  Usage:      encrypt, verify, wrap

Certificate Object, type = X.509 cert
  label:  Test
  ID:     45
```

, :

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -r -y cert  --id {id} > __.crt
```

{id} ID

```
Using slot 0 with a present token (0x0)
```

, . .

:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so --label "_" --keypairgen --key-type rsa:2048 -l --id 45
```

:

openssl

```
OpenSSL> engine dynamic -pre SO_PATH:/usr/lib/x86_64-linux-gnu/engines-1.1/pkcs11.so -pre ID:pkcs11 -pre LIST_ADD:1  -pre LOAD -pre MODULE_PATH:/usr/lib/librtpkcs11ecp.so
```

```
(dynamic) Dynamic engine loading support
[Success]: SO_PATH:/usr/lib/x86_64-linux-gnu/engines-1.1/pkcs11.so
[Success]: ID:pkcs11
[Success]: LIST_ADD:1
[Success]: LOAD
[Success]: MODULE_PATH:/usr/lib/librtpkcs11ecp.so
Loaded: (pkcs11) pkcs11 engine
```

⚠ Astra Linux SE 1.6 pkcs11 libengine-pkcs11-openssl 1.0.2 librtpkcs11ecp.so. , libengine-pkcs11-openssl1.1 0.4.4-4 Astra Linux Special Edition 10015-01 (1.6): libengine-pkcs11-openssl_1.0.4-4_amd64.deb

```
OpenSSL> req -engine pkcs11 -new -key 0:45 -keyform engine -x509 -out __.crt -outform DER
```

```
engine "pkcs11" set.
Enter PKCS#11 token PIN for Rutoken ECP <no label>:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Moscow
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Rusbitech
Organizational Unit Name (eg, section) []: Astra
Common Name (e.g. server FQDN or YOUR name) []:Makhmadiev Shuhrat
Email Address []:shuhrat@astralinux.ru

OpenSSL> exit
```

⚠️ 1) pkcs11.so

pkcs11.so :

```
find /usr/*(lib|lib64) -name pkcs11.so
```

2) .. , openssl ⚠️ openssl .

, :

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -l -y cert -w __.crt -a "___"
--id 45
```

:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -O
```

```
Using slot 0 with a present token (0x0)
Public Key Object; RSA 2048 bits
  label:      _
  ID:         45
  Usage:      encrypt, verify, wrap
Certificate Object, type = X.509 cert
  label:      ___
  ID:         45
```

Astra Linux

- -

:

- libccid
- pcscd
- libpam-p11
- libpam-pkcs11
- libp11-2
- libengine-pkcs11-openssl
- opensc

FLY:

```
sudo apt install opensc libengine-pkcs11-openssl libp11-2 libpam-pkcs11 libpam-
p11 pcscd libccid
```

openssl

```
OpenSSL> x509 -in __.crt -out cert.pem -inform DER -outform PEM
```

cert.pem -

ID :
:

```
mkdir ~/.eid
chmod 0755 ~/.eid
cat ___.pem >> ~/.eid/authorized_certificates
chmod 0644 ~/.eid/authorized_certificates
```

, :

```
mkdir /home/user/.eid
chmod 0755 /home/user/.eid
cat ___.pem >> ~/.eid/authorized_certificates
chmod 0644 /home/user/.eid/authorized_certificates
```

, , id.

- - Fly

```
sudo nano /usr/share/pam-configs/p11
```

:

```
Name: Pam_p11
Default: yes
Priority: 800
Auth-Type: Primary
Auth: sufficient pam_p11_opensc.so /usr/lib/librtpkcs11ecp.so
```

, Alt + X, Y, :

```
sudo pam-auth-update
```

Pam_p11 OK

- - Fly

```
sudo login
```

. Login , Password <PIN >. , , <PIN >.

libpam-pkcs11 pkcs11_eventmgr, PKCS#11.

pkcs11_eventmgr - /etc/pam_pkcs11/pkcs11_eventmgr.conf

:

```
pkcs11_eventmgr
{
    #
    daemon = true;

    #
    debug = false;

    #
    polling_time = 1;

    #  -
    # - 0
    expire_time = 0;

    #  pkcs11
    pkcs11_module = /usr/lib/librtpkcs11ecp.so;

    #
    #  :
    event card_insert {
        #     (  )
        on_error = ignore ;

        action = "/bin/false";
    }

    #
    event card_remove {
        on_error = ignore;

        #
        action = "fly-wmfunc FLYWM_LOCK";
    }

    #
    event expire_time {
        #     (  )
        on_error = ignore;

        action = "/bin/false";
    }
}
```

pkcs11_eventmgr .

---

pkcs11-tool:

```
$ pkcs11-tool --slot 0 --init-token --so-pin '87654321' --label '__' --module
/usr/lib/librtpkcs11ecp.so
```

:

```
pkcs15-init --erase-card
pkcs15-init --create-pkcs15 --so-pin "87654321" --so-puk ""
pkcs15-init --store-pin --label 'User PIN' --auth-id 02 --pin '12345678' --puk
'' --so-pin '87654321' --finalize
```

(rtAdmin)

rtAdmin : , PIN- , Flash-.

.

- Lite
- Lite SC
-
- 2.0
- SC
- PKI
- Flash
- 2.0 Flash/touch
- PINPad

:

rtadmin.zip

https://dev.rutoken.ru/pages/viewpage.action?pageId=7995615

1. (-q)

   ```
   ./rtadmin -f -q
   ```

2. , RutokenLabel, PIN- 123456789 PIN- 987654321.

   ```
   ./rtadmin -f -z /usr/lib/librtpkcs11ecp.so -L RutokenAstra -u 123456789 -a 98765432
   1 -q
   ```

:

1		-f	-
2	PIN-	-o [PIN- (32)]	87654321 -o
3	PIN-	- [PIN- (32)]	12345678 -c
4	PIN-	-a [PIN- (32)]	87654321 -a
5	PIN-	-u [PIN- (32)]	12345678 -u
6	PIN2- (PINPad.)	-t	-

7	PIN- ( )	-G [PIN- (8-32)]	-
8	PIN- ( )	-g [PIN- (8-32)]	-
9	PIN-	-b [ ]	-
10	PIN-	-p [PIN-: 1 – , 2 – , 3 –]	2
11	PIN-	-M [PIN- (6-31 Lite, 1 S)]	6
12	PIN-	-m [PIN- (6-31 Lite, 1 S)]	6
13	PIN-	-R [(3-10)]	10
14	PIN-	-r [(1-10)]	10
15	Windows-1251	-L [ ]	-
16	UTF-8	-D [ ]	-
17	UTF-8 (, PIN-)	-U	PIN- UTF-8
18		-q	-
19	PKCS#11	-z [ ]	librtPKCS11ecp.so
20		-n [ ]	-
21		-l [ ]	: , : rtadmin.log

Web

(https://www.rutoken.ru/products/all/rutoken-plugin/) – .

.

, ,

:

https://rutoken.ru

- .

https://dev.rutoken.ru

.

https://kb.rutoken.ru/display/kb

,

. .

https://forum.rutoken.ru

.

.

:

https://dev.rutoken.ru/pages/viewpage.action?pageId=78479384

:

https://www.rutoken.ru/support/feedback

:

https://help.rutoken.ru
e-mail:
hotline@rutoken.ru
.: +7 495 925-77-90